receive a request for information from the client device using the anonymous identifier and random identifiers;

send the queued breach alert message for each random identifier that includes the breach alert message to the client device based on the anonymous identifier.

14. The system of claim **10** where:

in receiving the breached web data elements, the breached web data elements are breached passwords and the breached passwords are hashed to generate breached password hashes; and

in receiving the at least one user login data hash, the at least one user login data hash comprises at least one password hash, and the hashed user login data hash comprises a hashed password hash.

15. The system of claim **14** where:

the breached web data elements include breached username-password combinations and corresponding domain names where the breached username-password combinations are hashed to generate breached username-password hashes, hashing the breached web data hashes includes hashing the breached username-password hashes using the hashing method with the non-exportable key, and the breach detection module is configured to:

receive at least one username-password combination hash from the client device processed using the hashing method, where no information associated with a user of the client device user is received from the client device;

hash the at least one username-password combination hash using the hashing method and the non-exportable key to generate a hashed username-password combination hash for each username-password combination hash;

compare each hashed username-password combination hash with each of the hashed breached username-password hashes;

send a breach notification to the client device for each hashed username-password combination hash that matches one of the hashed breached username-password hashes, where the breach notification includes the domain name corresponding to the matching breached username-password combination; and

store the anonymous identifier and each hashed username-password combination hash that does not match any of the hashed breached username-password combinations.

16. The system of claim **10** where:

in receiving the breached web data elements, the breached web data elements include breached username-password combinations where the breached username-password combinations are hashed to generate breached username-password hashes;

hashing the breached web data hashes includes hashing the breached username-password hashes using the hashing method with the non-exportable key;

in receiving the at least one user login data hash, the at least one user login data hash includes at least one username-password combination hash;

hashing the at least one user login data hash includes hashing the at least one username-password combination hash.

17. The system of claim **10** where:

in receiving the breached web data elements, the breached web data elements include breached usernames and the breached usernames are hashed to generate breached username hashes;

hashing the breached web data hashes includes hashing the breached username hashes using the hashing method with the non-exportable key;

in receiving the at least one user login data hash, the at least one user login data hash includes at least one username hash;

hashing the at least one user login data hash includes hashing the at least one username hash.

18. The system of claim **10** where the HSM performs the hashing method using the HMAC-SHA512 as the hashing method.

19. The system of claim **10** where the web breached data comprises dark web breached data provided by breached data providers.

* * * * *